BAB II

TINJAUAN PUSTAKA

A. Tindak Pidana *Cyber Crime*

Tindak pidana *cyber crime* merupakan objek dari penelitian ini, maka dalam bab ini perlu dijabarkan bagaimana tinjauan umum dari tindak pidana cyber crime.

a. Pengertian *Cyber Crime*

Memasuki pembahasan terkait pengertian cyber crime maka akan menyinggung tentang keamanan suatu jaringan komputer atau informasi teknologi telekomunikasi. Terutama pada era globalisasi saat ini, yang membawa kemajuan teknologi sangat pesat maka hal tersebut tidak terlepas adanya resiko dari penyalahgunaan dari pemanfaatan teknologi sebagai kebutuhan informasi.

> "Teknologi telekomunikasi telah membawa manusia kepada suatu peradaban baru dengan struktur sosial beserta tata nilainya.Artinya, masyarakat berkembang menuju masyarakat baru yang berstruktur global.Sistem tata nilai dalam suatu masyarakat berubah, dari yang bersifat lokal-partikular menjadi global universal. Hal ini pada akhirnya akan membawa dampak pada pergeseran nilai, norma, moral, dan kesusilaan." [10]

Kemajuan teknologi sangat berdampak besar bagi masyarakat yang membawa dampak positif dan dampak negatif terhadap perkembangan manusia dan peradabannya. Dampak negatif yang dimaksud adalah yang berkaitan dengan dunia kejahatan. J. E Sahetapy telah

[10] Abdul Wahid dan Mohammad Labib, 2005, *Kejahatan Mayaantara (Cybercrime)*, Bandung, PT Refika Aditama, hlm. 23.

menyatakan, bahwa kejahatan erat kaitanya dan bahkan menjadi sebagian dari hasil budaya itu sendiri. Maka demikian artinya semakin tinggi tingkat budaya dan semakin modern suatu bangsa, maka semakin modern pula kejahatan itu dalam bentuk, sifat dan cara pelaksanaanya.[11]

Perkembangan teknologi komputer, teknologi informasi, dan teknologi komunikasi juga menyebabkan munculnya tindak pidana baru yang memiliki karakteristik yang berbeda dengan tindak pidana konvensional. Penyalahgunaan komputer sebagai salah satu dampak dari ketiga perkembangan teknologi tersebut itu tidak terlepas dari sifatnya yang memiliki ciri-ciri tersendiri sehingga membawa persoalan yang rumit dipecahkan berkenaan dengan masalah penanggulangannya mulai dari penyelidikan, penyidikan hingga dengan penuntutan.[12]

Sehingga berdasarkan beberapa pendapat tersebut maka dapat dikatakan bahwa adanya kemajuan teknologi dan informasi selain dapat dipergunakan manusia sebagai komoditi informasi, juga dapat membawa dampak negatif yakni penyalahgunaan teknologi yang membawa hal tersebut pada suatu tindak pidana yang disebut dengan *cyber crime*. Adapun tindak pidana cyber crime ini memiliki karakteristik tersendiri karena berhubungan dengan jaringan teknologi

[11] J. E Sahetapy dalam Abdul Wahid, 2002, *Kriminologi dan Kejahatan Kontemporer*, Lembaga Penerbitan Fakultas Hukum Unisma, Malang

[12]Edmon Makarim, 2005, *Pengantar Hukum Telematika (Suatu Kajian Kompilasi)*, Jakarta PT Raja Grafindo Persada, hlm. 426.

komputer sehingga dalam penangannya tidak dapat disamakan dengan tindak pidana konvensional.

Cybercrime merupakan kejahatan yang berbeda dengan kejaharan konvensional (*street crime*). *Cyber crime* muncul bersamaan dengan lahirnya revolusi teknologi informasi. Sebagimana dikemukakan oleh Ronni R. Nitibaskara bahwa: "Interaksi sosial yang meminimalisir kehadiran secara fisik, merupakan ciri lain revolusi teknologi informasi. Penyimpangan social menyesuasikan bentuk dn karakter baru dalam kejahatan.[13]

Merujuk pada pendapat tersebut maka *cyber crime* dapat dimaknai secara luas dan sempit. Dalam arti sempit, *cyber crime* dapat dimaknai sebagai perbuatan yang melanggar hukum dengan memanfaatkan teknologi komputer. Sedangkan dalam arti luas, *cyber crime* merupakan keseluruhan bentuk kejahatan yang ditujukan pada komputer baik dari jaringan maupun penggunanya serta kejahatan konvensional yang menggunakan teknologi komputer.

Cyber crime atau kejahatan dunia maya dalam peraturan Perundang-undangan di Indonesia juga sering disebut dengan kejahatan tindak pidana yang berkaitan dengan teknologi informasi, hal ini sejalan dengan pengertian yang diberikan oleh Donn B. Parker yang memberikan definisi sebagai berikut.

[13]Ronni R Nitibaskara dalam Didik M. Arief Mansur dan Elisatris Gultom, 2005, *Cyber Law Aspek Hukum Teknologi Informasi*, Bandung, PT Refika Aditama, hlm. 25.

> "*Computer abuse is broadly defined to be any incident associated with computer technology in which a victim suffered or could suffered loss and a perpetrator by intention made or could have gain*", yang kemudian diterjemahkan oleh Andi Hamzah sebagai penyalahgunaan komputer didefinisikan secara luas sebagai suatu kejadian yang berhubungan dengan teknologi komputer yang seorang korban menderita atau akan telah menderita kerugian dan seorang pelaku dengan sengaja memperoleh keuntungan atau akan telah memperoleh keuntungan".[14]

Sehingga tindak pidana *cyber crime* adalah suatu tindak pidana yang dilakukan dengan menggunakan jaringan teknologi informasi komputer untuk mendapatkan data secara ilegal serta dipergunakan untuk mengambil keuntungan yang tidak sah dan menyebabkan kerugian pada masyarakat.

b. Dasar Hukum Cyber Crime

Sebelum membahas definisi dari tindak pidana cyber crime, terlebih dahulu akan dijabarkan terkait dengan dasar hukum dari cyber crime itu sendiri. Adapun dasar hukum yang mengatur tentang tindak pidana cyber crime adalah sebagai berikut.

1. Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi mengatur beberapa pasal yang memuat tentang perbuatan yang dilarang termasuk tindak pidana *cyber crime*. Undang-Undang Nomor 36 Thn 1999 tentang Telekomunikasi diberlakukan untuk mengakomodir pemidanaan dari tindak pidana

[14] Andi Hamzah, 1993, *Hukum Pidana yang berkaitan dengan komputer*, Jakarta : Sinar Grafika Offset, hal. 18

cyber crime, sebelum lahirnya Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Namun Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi ini hanya mengatur beberapa tindak pidana yang termasuk tindak pidana cybercrime yang masih bersifat umum dan luas, dan hanya berkaitan dengan telekomunikasi, sehingga belum dapat mengakomodir tindak-tindak pidana yang berkaitan dengan komputer. Adapun beberapa pasal tersebut yakni sebagai berikut.

Tabel 1
Pengaturan Cyber crime dalam Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Pasal	Materi
Pasal 22	dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi : Akses ke jaringan telekomunikasi; dan atau Akses ke jasa telekomunikasi; dan atau Akses ke jaringan telekomunikasi khusus
Pasal 38	dilarang melakukan perbuatan yang dapat menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi
Pasal 40	dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun

Sumber: Undang-Undang Nomor 36 Thn 1999 tentang Telekomunikasi

Selain dari pasal-pasal tersebut, bentuk-bentuk tindak pidana *cyber crime* yang disebutkan dalam Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi adalah akses

illegal. Akses ilegal yakni tanpa hak, tidak sah, atau memanipulasi akses ke jaringan telekomunikasi, menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi dan penyadapan informasi melalui jaringan telekomunikasi.

2. Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik diundangkan pada tanggal 23 April 2008. Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik memuat dan mengakomodir tentang pengelolaan informasi dan transaksi elektronik untuk pembangunan, dan juga sebagai antisipasi atau payung hukum dari resiko buruk jika terdapat penyalahgunaan kemajuan teknologi informasi dan transaksi elektronik yang dapat merugikan kepentingan hukum baik bagi orang pribadi, masyarakat ataupun negara yang menggunakan alat teknologi atau dengan kata lain yang dapat disebut dengan tindak pidana *cyber crime*.

Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik telah menetapkan perbuatan-perbuatan mana yang termasuk tindak pidana di bidang *cyber crime* dan telah ditentukan unsur-unsur tindak pidana dan penyerangan terhadap berbagai kepentingan hukum dalam bentuk rumusan-rumusan

tindak pidana tertentu. Adapun pasal-pasal yang mengatur tindak pidana cyber crime adalah sebagai berikut.

Tabel 2
Pengaturan Cyber crime dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Pasal	Materi
Pasal 27 ayat (1)	Dengan sengaja atau tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan
Psl 27 ayat (2)	Dengan sengaja tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian
Psl 27 ayat (3)	tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atauDokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik
Psl 27 ayat (4)	tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman
Psl 28 ayat (1)	tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik
Psl 28 ayat (2)	tanpa hak menyebarkan yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antar golongan (SARA).

Pasal 29	tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi
Pasal 30 ayat (1)	tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun
Pasal 30 ayat (2)	tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik
Pasal 30 ayat (3)	tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan
Pasal 31ayat (1)	tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain
Pasal 31ayat (2)	tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.
Pasal 31ayat (3)	Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang

	ditetapkan berdasarkan undang-undang
Pasal 32 ayat (1)	tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik public
Pasal 32 ayat (2)	tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak
Pasal 32 ayat (3)	Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.
Pasal 33	tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.
Pasal 34 ayat (1)	tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki: a) perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untukmemfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33 b) sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai

	dengan Pasal 33
Pasal 34 ayat (2)	Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hokum
Pasal 35	tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik
Pasal 36	tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.
Pasal 37	dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia

Sumber: Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Berdasarkan penjelasan tersebut, maka pasal yang mengatur secara jelas terkait penyadapan adalah pasal 31 ayat (1) tentang penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain, lalu dilanjutkan dengan pasal 31 ayat (2) yakni penyadapan baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen

Elektronik yang sedang ditransmisikan. Lebih lanjut lagi dalam pasal 31 ayat (3) penyadapan diperbolehkan jika dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.

3. **Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik**.

Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik merupakan bentuk dari perubahan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Namun terkait dengan bentuk-bentuk dari tindak pidana cyber crime yang diatur tidak ada perubahan, sehingga segala bentuk tindak pidana cyber crime masih sama halnya dengan yang diatur dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

a. Bentuk-Bentuk Tindak Pidana *Cyber Crime*

Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur bentuk- bentuk tindak pidana *cyber crime* yang tercantum dalam psl 27 sampai dengan psl 35 UU No11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, diantaranya yakni.

1) *Cybercrime* yang menggunakan komputer sebagai alat kejahtan, yakni Pornografi Online (*Cyber-Porno*), Perjudian Online, Pencemaran nama baik melalui media sosial, penipuan melalui komputer, pemalsuan melalui komputer,pemerasan dan pengancaman melalui komputer, penyebaran berita bohong melalui komputer, pelanggaran terhadap hak cipta, *cyber terrorism*
2) *Cybercrime* yang berkaitan dengan komputer, jaringan sebagai sasaran untuk melakukan kejahatan, yakni akses tidak sah (*illegal acces*), menggangu sistem komputer dan data komputer, penyadapan atau intersepsi tidak sah, pencurian data, dan menyalahgunakan peralatan komputer.

Dari penjelasan tersebut dapat ditarik bahwa tindak pidana cybercrime berdasarkan bentuknya dapat dibedakan secara dua garis besar. Pertama, cybercrime yang menggunakan komputer sebagai sarana atau alat dalam melakukan pidana seperti pencemaran nama baik melalui media sosial, penyeberan berita hoax di media masa, dan lain-lain. Sedangkan yang kedua adalah cybercrime dengan komputer sebagai sasaran kejahatan yakni hacking, penyadapan, pencurian data komputer secara ilegal dan lain-lain.

B. Informasi Elektronik

Menurut psl 1 ayat (1) UU No 11 Thn 2008 tentang Informasi dan Transaksi Elektronik menyatakan informasi elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang

telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Berdasarkan psl tersebut maka dapat dikatakan bahwa segala informasi yang berbentuk elektronik Jonner Hasugian dalam artikelnya berpendapat bahwa dalam era saat ini berbagai sumber daya informasi yang berbasis pada kertas telah tersedia dalam format elektronik.[15]

Kemudian dalam pasal 4 Undang-Undang Nomor 11 Thn 2008 tentang Informasi dan Transaksi Elektronik bahwa Pemanfaatan Teknologi Informasi dan Elektronik dilaksanakan dengan tujuan untuk:

a) mencerdaskan kehidupan bangsa sebagai bagian dari masyarakat informasi dunia;
b) mengembangkan perdagangan dan perekonomian nasional dalam rangka meningkatkan kesejahteraan masyarakat; meningkatkan efektivitas dan efisiensi pelayanan publik;
c) membuka kesempatan seluas-luasnya kepada setiap orang untuk memajukan pemikiran dan kemampuan di bidang penggunaan dan pemanfaatan Teknologi Informasi seoptimal mungkin dan bertanggung jawab;
d) dan memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara Teknologi Informasi.

[15] Jonner Hasugian. 2008. *Urgensi Literasi Informasi dalam Kurikulum Berbasis Kompetensi di Perguruan Tinggi. Jurnal Studi Perpustakaan dan Informasi*, Vol. 4, No. 2, Desember 2008.

C. Transaksi Elektronik

Berdasarkan pasal 1 ayat 2 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik bahwa pengertian transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya. Perbuatan hukum merupakan perbuatan yang dilakukan subjek hukum dan bertujuan untuk menimbulkan akibat hukum yang dikehendaki, yakni hak dan kewajiban yang melekat pada pihak yang melakukan dalam hal ini adalah pelaku usaha dan konsumen.[16]

Selanjutnya dalam pendapat ahli, perkembangan teknologi yang didorong adanya konvergensi antara teknologi telekomunikasi dan informatika dan termasuk lahirnya terobosan baru bagi kegiatan bisnis yang disebut dengan perdagangan elektronik atau dengan kata lain *e-commerce*.[17]

Transaksi elektronika adalah setiap transaksi yang dilakukan oleh dua pihak atau lebih melalui jaringan komputer atau media elektronik lainnya, dengan menggunakan sistem informasi elektroika yang menimbulkan hak dan kewajiban kepada masing-masig pihak yang bertransaksi.[18]

Sehingga berdasarkan pada pendapat tersebut maka dapat diambil kesimpulan bahwa transaksi elektronik adalah suatu perbuatan hukum dan

---

[16] Enni Soerjati. 2014. *Pengaturan Transaksi Elektronik dan Pelaksanannya di Indonesia dikaitkan dengan Perlindungan E-Konsumen*. Padjajaran Jurnal Ilmu Hukum Volume 1 Nomor 2.

[17] *Ibid.*

[18] Inca panjaitan., dkk.. 2005. *Membangun Cyberlaw Indonesia yang Demokratis*. Jakarta : IMPLC. Hal. 87

dapat berupa kegiatan bisnis atau perdagangan yang dilakukan melalui teknologi komputer, jaringan komputer atau media elektronik lainnya.

D. Penyadapan

Berdasarkan penjelasan pasal 1 ayat 2 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, penyadapan atau intersepsi adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan atau mencatat transmisi informasi elektronik dan atau Dokumen elektronik yang bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti elektromagnetis atau Radio.

Sedangkan istilah penyadapan menurut *Blacks Law Dictionary* menjelaskan *"intercept'* sebagai *"to covertly receive or listen to (a communication). The term usu. refers to covert reception by a law-enforcement agency' yang identik dengan istilah "wiretapping" yang berarti "electronic or mechanical eavesdropping, usu. done by law-enforcement officers under court order, to listen to private conversation"*[19] Berdasarkan pada definisi tersebut dapat diambil ciri-ciri dari penyadapan adalah pengambilan data secara diam-diam/ tanpa sepengetahuan pihak lain.

Sedangkan dalam penjelasan pasal 40 undang-undang Republik Indonesia Nomor 36 Tahun 1999 tentang Telekomunikasi, penyadapan yakni kegiatan memasang alat atau perangkat tambahan pada jaringan

[19] Bryan A. Gamer, ed.2004. *Block's Low Dictionary, Thomson West, Elgth Edition, St.Paul Minnesota*. Hal.827

telekomunikasi untuk tujuan mendapatkan informasi dengan cara tidak sah. Pada dasarnya informasi yang di miliki oleh seseorang adalah hak pribadi yang harus di lindungi sehingga penyadapan harus di larang.

Sehingga berdasarkan pada kedua bunyi pasal tersebut dapat diambil kesimpulan bahwa penyadapan adalah kegiatan mendapatkan informasi . untuk mendengarkan, membelokkan, atau bahkan menghambat dengan menggunakan jaringan telekomunikasi.

Pada Undang-Undang Nomor 36 tahun 1999 tentang telekomunikasi mengatur tindak pidana penyadapan bukan hanya sebagai tindak pidana namun penyadapan juga dapat dikategorikan sebagai tindak penyiidikan untuk keperluan proses peradilan pidana. Kemudian setelah lahir Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, penyadapan diatur dalam pasal 31 yang menyatakan

> (1) "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain".
> (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.

Melihat pada bunyi pasal tersebut bahwa pasal 31 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur penyadapan secara luas atau secara umum.

Sedangkan pasal 31 ayat (2) Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur penyadapan pada transmisi informasi elektronik/dokumen elektronik.

E. Tindak Pidana *Carding*

Pada penelitian ini akan membahas terkait dengan Upaya Kepolisian dalam Menanggulangi Tindak Pidana Carding.

a. Pengertian *Carding*

Tindak pidana *Carding* merupakan bagian dari tindak pidana *cyber crime* , yakni tindak pidana yang menggunakan kartu kredit milik orang lain yang diperoleh secara illegal dan digunakan untuk mengambil keuntungan pribadi.

Tindak pidana *carding* dapat dilakukan dengan beberapa modus kejahatan. Mulai dari pelaku membuat identitas palsu untuk aplikasi kartu kredit samoai dengan membuat kartu kredit palsu yang menggunakan teknologi canggih dalam menerbitkan kartu kredit.[20] Pelaksanaan modus operandi tersebut juga didukung berbagai instrumen seperti skimmer atau software untuk generate nomor kartu kredit dan kesempatan yang relatif terbuka untuk mencuri data dari kartu kredit seperti di hotel, restaurant, card centre dll. sehingga identitas kartu kredit dapat diperoleh dengan mudah.[21]

---

[20] Sigid Suseno dan Syarif A. Barmawi. *Kebijakn Pegaturan Carding dalam Hkm Pidana di Indones*ia. Jurnal Sosiohumaniora, Vol. 6, No. 3. Hal 253.

[21] VISA International, 2002. *Credit Card Fraud Trend & Legislation*, Bandung,Hal.13.

Penipuan kartu kredit adalah masalah yang sedang menjadi trend di dunia maya modern ini. Jumlah total penipuan kartu kredit pada tahun 1982, termasuk yang melibatkan kartu bank, kartu toko ritel, dan kartu gas, kira-kira satu miliar dolar, dan kerugian tahunan segera bisa mencapai dua miliar dolar.[22] Tentunya, kerugian ini ditanggung oleh konsumen atau pemegang kartu kredit.

Tindak pidana *carding* merupakan kejahatan yang membawa resiko sangat besar bagi masyarakat, sehingga untuk menyikapi hal tersebut maka penegak hukum diberikan pelatihan untuk menangani kasu-kasus dari teknik penyelidikan, penyidikan dan pengamanan untuk menangani kejahatan dalam bidang elektronik akan tetapi kemampuan hukum untuk menanggulangi kejahatan mengalami penurunan, hal ini dikarenakan struktur hukum dengan fungsi hukum tidak berkembang secara paralel sehinga penegakan hukum cenderung terus melemah.[23]

Adapun beberapa modus yang dapat dilakukan oleh pelaku adalah sebagai berikut.[24]

a. *Fraud application*; Menggunakan kartu kredit asli yang diperoleh dengan aplikasi palsu. Pelaku memalsu data pendukung dalam proses aplikasi seperti : KTP, Pasport, rekening koran, Surat Keterangan Pengahsilan dll.
b. *Non received card*; Menggunakan kartu kredit asli yang tidak diterima oleh oleh pemegang kartu kredit yang sah (berhak) kemudian pelaku membubuhkan tanda tangan di kolom tanda tangan. Kartu kredit diperoleh melalui kurir atau membobol kantos pos bila dikirim melalui Pos.

[22] *Journal of Criminal Law and Criminology*, Volume 76, Isuue 3, Article 7, hal. 3
[23] Mahfud M.D, 2000, *Poitik Hukum Nasional*, Bandung: Alumni . Hal. 35
[24] Sigid Suseno dan Syarif A. Barmawi. Op.cit. Hal 254

c. *Lost/stolen card*; Menggunakan kartu kredit asli hasil curian atau hilang. Pada waktu melakukan transaksi pelaku menandatangani sales draft dan meniru tanda tangan pada kartu kredit atau tanda tangan pemegang kartu yang sah. Transaksi dilakukan di bawah floor limit agar tidak perlu dilakukan otorisasi.
d. *Altered card*; Menggunakan kartu kredit asli yang sudah diubah datanya. Pelaku menggunakan kartu hasil curian (lost/stolen, non received, expired card) dan kartu reliefnya dipanasi dan diratakan kemudian direembossed dengan data baru. Sedangkan magnetic stripe diisi data baru dengan reencoded yang diperoleh dari point of compromise (POC).
e. *Totally counterfeited*; Menggunakan kartu kredit yang seluruhnya palsu. Pelaku mencetak kartu tiruan dengan menggunakan data nomor dan pemegang kartu yang masih berlaku dengan melakukan reembossed dan reencoded.
f. *White plastic card*; Menggunakan kartu plastik polos yang berisi data asli. Pelaku mencetak data dari pemegang kartu kredit yang sah pada plastik polos, tanpa meniru hologram dan logo penerbit. Magnetic stripe diisi dengan data pemegang kartu dengan cara encoding.
g. *Record of charge (Roc) pumping*; Penggandaan sales draft oleh merchant (pedagang). Sales draft yang satu tidak ditandatangi oleh pemegang kartu yang sah dan diserahkan kepada merchant lain untuk diisi dengan data transaksi fiktif.
h. *Altered amount*; Mengubah nilai transaksi pada sales draft oleh merchant (pedagang).
i. *Telephone/mail ordered*; Memesan barang melalui telepon atau surat dengan menggunakan kartu kredit orang lain yang sudah diketahui nama dan nomornya.
j. *Mengubah program Electronic Data/Draft Capture* (EDC); Mengubah dan merusak program pada alat otorisasi (electronic data/draft capture/EDC) milik pengelola oleh merchant (pedagang).
k. *Fictius merchant*. Pelaku berpura-pura menjadi pedagang dengan mengajukan aplikasi disertai dengan data-data palsu.

Sehingga berdasarkan pada beberapa modus yang dapat dilakukan untuk melakukan kejahatan *carding* mulai dari menggunakan aplikasi

hacking untuk mencuri beberapa data milik pengguna kredit untuk verifikasi, menggunakan kartu kredit curian, bahkan pelaku dapat menggandakan file yang berisikan data transaksi fiktif.

b. Dasar Hukum *Carding*

Pengaturan tentang tindak pidana *carding* diatur dalam ketentuan perundang-undangan sebagai berikut.

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Carding dapat ditangani dengan beberapa pasal yang ada dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Elektronik. Dalam melakukan tindak pidana *carding* , pelaku dapat melakukan *hacking* untuk mendapatkan beberapa data dan informasi yang akan digunakan pelaku untuk mengambil keuntungan. Sehingga hal tersebut dapat dijerat dengan pasal 31 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Elektronik yang menyatakan "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronika dan atau dokumen elektronik dalam suatu komputer dan atau sistem elektronik secara tertentu milik orang lain". Dan pasal 31 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Elektronik yang menyatakan Setiap orang dengan sengaja atau tanpa hak atau melawan hukum melakukan intersepsi atau transmisi elektronik dan atau dokumen elektronik

yang tidak bersidat publik dari, ke dan di dalam suatu komputer dan atau sistem elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan, penghilangan dan atau penghentian informasi elektronik dan atau dokumen elektronik yang ditransmisikan.

2. Kitab Undang- Undang Hukum Pidana

Tindak pidana *carding* dapat dikaitkan dengan pasal pencurian, tindak pidana pemalsuan dan pidana penipuan yang terdapat dalam Kitab Undang- Undang Hukum Pidana yakni dalam pasal sebagai berikut.[25]

1. Pasal 362 KUHP yang menyatakan "Barang siapa mengambil suatu benda yang seluruhnya atau sebagian milik orang lain, dengan maksud untuk dimiliki secara melawan hukum".
2. Pasal 378 KUHP "Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain dengan melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat ataupun dengan rangkaian kebohongan menggerakkan orang lain untuk menyerahkan sesuatu benda kepadanya, atau supaya memberi hutang maupun menghapuskan piutang."

Sehingga sebelum lahirnya Undang- undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, para penegak

[25] Kurniawan. 2006. *Penegakan Hukum Tindak Pidana Kartu Kredit*. Skripsi. Unair di akses 01 april 2019 pukul 20.00 WIB

hukum menggunakan pasal 362 dan pasal 378 KUHP untuk menjerat pelaku, namun tentunya karakteristik dari tindak pidana *carding* yang menggunakan teknologi berbeda dengan tindak pidana konvensional.

F. Penyidikan

Penyidikan jika didasarkan pada istilah kata dapat didefinisikan sebagai *investigation* dalam bahasa Inggris, *opsporing* dalam bahasa Belanda dan *penyiasatan* dalam bahasa Malaysia.[26] Sedangkan menurut pasal 1 ayat 2 Kitab Undang- Undang Hukum Acara Pidana, penyidikan adalah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam uu utk mengumpuulkan butki guna menemukkan pelakunya.

Kemudian penyidikan juga didefinisikan oleh M. Yahya Harahap sebagai berikut.

> Suatu tindakan lanjutdari kegiatan penyelidikan dengan adanya suatu terjadinya peristiwa tindakpidana. Persyaratan dan pembatasan yang ketat dalam penggunaan upaya paksasetelah pengumpulan bukti permulaan yang cukup guna membuat terang suatuperistiwa yang patut diduga merupakan tindak pidana.[27]

Sedangkan menurut De Pinto, penyidikan memiliki definisi

> Pemeriksaan permulaan olehpejabat-pejabat yang untuk itu ditunjuk oleh undang-undang segera setelahmereka dengan jalan apa pun mendengar kabar yang sekedar beralasan, bahwaada terjadi sesuatu pelanggaran hukum.[28]

---

[26] Andi Hamzah. 2008. *Hukum Acara Pidana Indonesia*. Jakarta : Sinar Grafika. Hal. 120.

[27] M Yahya Hhrp. 2006. *Pembahasan Permasalahan Dan Penerapan KUHAP :Penyidikan Dan Penuntutan*. Jakarta : Sinar Grafika. Hal. 210.

[28] *Ibid.*

Sehingga berdasarkan pembahasan tersebut dpat diambil kesimpulan bahwa penyidikan adalah serangkaian tindakan yang dijalankan oleh penyidik dengan mengumpulkan bukti untuk membuat terang suatu tindak pidana dan untuk menemukan tersangka.

G. Kepolisian

Pasal 1 ayat (1) UU No 2 Thn 2002 tentang Kepolisian Negara Republik Indonesia menjelaskan bahwa Kepolisian adalah segala hal-ihwal yang berkaitan dengan fungsi dan lembaga polisi sesuai dengan peraturan perundang-undangan. Jadi kepolisian menyangkut semua aspek yang berkaitan dengan tugasdan wewenang kepolisian serta kelembagaan yang ada di dalamnya.

Sedangkan dalam pasal 13 UU No 2 Thn 2002 tentang Kepolisian Negara Republik Indonesia, menjelaskan bahwa tugas pokok dari Kepolisian Negara Republik Indonesia adalah

a.memelihara keamanan dan ketertiban masyarakat;
b.menegakkan hukum; dan
c.memberikan perlindungan, pengayoman, dan pelayanan kepada masyarakat

Kemudian penjabaran mengenai tugas pokok tersebut dijelaskan lebih lanjut dalam pasal 14 UU No 2 Thn 2002 tentang Kepolisian Negara Republik Indonesia yakni sebagai berikut.

a.melaksanakan pengaturan, penjagaan, pengawalan, dan patroli terhadap kegiatan masyarakat dan pemerintah sesuai kebutuhan;
b.menyelenggarakan segala kegiatan dalam menjamin keamanan, ketertiban, dan kelancaran lalu lintas di jalan;
c.membina masyarakat untuk meningkatkan partisipasi masyarakat, kesadaran hukum masyarakat serta ketaatan warga masyarakat terhadap hukum dan peraturan perundang-undangan;

d.turut serta dalam pembinaan hukum nasional;
e.memelihara ketertiban dan menjamin keamanan umum;
f.melakukan koordinasi, pengawasan, dan pembinaan teknis terhadap kepolisian khusus, penyidik pegawai negeri sipil, dan bentuk-bentuk pengamanan swakarsa;

Sehingga berdasarkan pada penjelasan pengertian dan tugas dari Kepolisian Negara Republik Indonesia bahwa sebuah lembaga yang menjalankan fungsi kepolisian sesuai dengan peraturan perundang-undangan yakni memelihara keamanan dan ketertiban, menegakkan hukum, dan melindungi dan mengayomi masyarakat.

H. Teori Efektivitas Hukum

Teori efektivitas hukum menurut Soerjono Soekanto adalah bahwa efektif atau tidaknya suatu hukum ditentukan oleh 5 (lima) faktor, yaitu:[29]

1. Undang- Undang

   Suatu hukum dapat dikatakan efektif juga ditentukan berdasarkan pada isi daripada peraturan hukum itu sendiri yang dapat berlaku secara yuridis, sosilogis dan juga filosofis.

2. Penegak Hukum

   Faktor yang kedua penegak hukum adalah pihak yang memnerpkaan hukum Namun untuk penegak hukum yang terlibat secara langsung diantaranya kepolisian, kejaksaan, kehakiman, kepengacaraan, dan pemasyarakatan.

[29] Riduan Syahrani. 2004. *Rangkuman Intisari Ilmu Hukum*. Banjarmasin. PT. Citra Aditya Bakti. Hal. 184.

3. Sarana atau Fasilitas

Sarana atau fasilitas tersebut, antara lain mencakup tenaga manusia yang berpendidikan dan terampil, organisasi yang baik, peralatan yang memadai, keuangan yang cukup, dan seterusnya.

4. Masyarakat

Semakin tinggi tinggi kesadaran masyarakat, maka akan semakin memungkinkan penegakan hukum yang baik.Sebaliknya, semakin rendah tingkat kesadaran hukum masyarakat, maka akan semakin sukar untuk melaksanakan penegakan hukum yang baik.

5. Kebudayaan

Kebudayaan pada dasarnya mencakup nilai nilai yang mendasari hukum yang berlaku, nilai nilai mana merupakan konsepsi abstrak mengenai apa yang dianggap baik dan apa yang dianggap buruk.